ИНФОРМАТИКА

2007 январь-март № 1

УДК 519.7

А.Д. Закревский

ДЕКОМПОЗИЦИЯ ЧАСТИЧНЫХ БУЛЕВЫХ ФУНКЦИЙ – ПРОВЕРКА НА РАЗДЕЛИМОСТЬ ПО ЗАДАННОМУ РАЗБИЕНИЮ

Рассматривается задача последовательной двухблочной декомпозиции частичных булевых функций по нестрогому разбиению на множестве аргументов. Предлагаются метод и алгоритм проверки функции на разделимость по заданному разбиению. При решении этой задачи используется аппарат булевых и троичных векторов и матриц с эффективными комбинаторными операциями над ними.

Введение

При рассмотрении проблемы декомпозиции булевых функций большое внимание уделяется последовательной двухблочной декомпозиции, в общем случае неразделительной, которая и рассматривается в данной статье.

В этом случае исходная булева функция $f(\boldsymbol{x})$, заданная на множестве аргументов $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$, заменяется композицией $g(h(\boldsymbol{u}, \boldsymbol{w}), \boldsymbol{w}, \boldsymbol{v})$ булевых функций g и h по некоторому нестрогому разбиению $\boldsymbol{u}/\boldsymbol{v}$, при котором $\boldsymbol{x} = \boldsymbol{u} \cup \boldsymbol{w} \cup \boldsymbol{v}$, $\boldsymbol{u} \cap \boldsymbol{w} = \boldsymbol{u} \cap \boldsymbol{v} = \boldsymbol{w} \cap \boldsymbol{v} = \varnothing$. Такая композиция иллюстрируется примером на рис. 1, где $\boldsymbol{u} = (x_1, x_2, x_3)$, $\boldsymbol{w} = (x_4, x_5)$ и $\boldsymbol{v} = (x_6, x_7)$. Заметим, что при этом должны выполняться неравенства $|\boldsymbol{u}| > 1$ и $|\boldsymbol{v}| > 0$, иначе декомпозиция тривиальна – существует всегда.

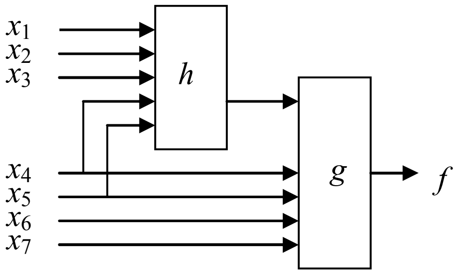

Рис. 1. Пример неразделительной последовательной двухблочной декомпозиции

В основе декомпозиционных методов лежит решение следующих двух задач.

Задача 1. Для заданных функции $f(\boldsymbol{x})$ и разбиения $\boldsymbol{u}/\boldsymbol{v}$ выяснить, декомпозируется ли $f(\boldsymbol{x})$ по $\boldsymbol{u}/\boldsymbol{v}$, т. е. существует ли композиция $g(h(\boldsymbol{u}, \boldsymbol{w}), \boldsymbol{w}, \boldsymbol{v})$, эквивалентная функции f, и, может быть, найти функции g и h.

Если такая композиция существует, назовем разбиение $\boldsymbol{u}/\boldsymbol{v}$ *подходящим*.

Задача 2. Для заданной функции $f(\boldsymbol{x})$ найти подходящее разбиение.

Решению этих задач посвящено множество публикаций. Например, в обзоре по данной проблеме [1], составленном еще в 1995 году, упоминаются 744 опубликованные работы. В частности, первая задача рассматривалась уже в работах [2, 3], вторая – в [4, 5].

В данной статье предлагается комбинаторный метод решения первой задачи для случая частичной булевой функции $f(\boldsymbol{x})$, определенной не на всех элементах булева пространства $M = \{0, 1\}^n$.

1. Представление данных и условие разделимости

Рассмотрим полностью определенную булеву функцию $f(\boldsymbol{x})$ и допустим, что $f(\boldsymbol{x}) = g(h(\boldsymbol{u}, \boldsymbol{w}), \boldsymbol{w}, \boldsymbol{v})$. В этом случае дизъюнктивное разложение Шеннона функции $f(\boldsymbol{x})$ по переменным множества $\boldsymbol{w}$ приводит к формуле

$$f(\boldsymbol{x}) = \bigvee_{k_i \in K_{\boldsymbol{w}}} k_i f_i ,$$

где $K_{\boldsymbol{w}}$ представляет множество всех полных элементарных конъюнкций над множеством переменных $\boldsymbol{w}$, а коэффициенты разложения f_i получаются в результате подстановки в функцию $f(\boldsymbol{x})$ вместо переменных, образующих множество $\boldsymbol{w}$, таких значений, которые обращают в единицу конъюнкцию k_i (обозначим эту операцию через $f(\boldsymbol{x})$: k_i). Число этих коэффициентов равно $2^{|\boldsymbol{w}|}$, и каждый из них зависит лишь от переменных множеств $\boldsymbol{u}$ и $\boldsymbol{v}$. Другими словами, $f_i = g_i(h_i(\boldsymbol{u}), \boldsymbol{v})$. Из этой формулы видно, что коэффициенты аналогичного дизъюнктивного разложения коэффициента f_i по переменным множества $\boldsymbol{u}$ должны принимать не более двух различных значений. Проверка этого условия была положена в основу ряда известных алгоритмов решения задачи 1.

В работе [6] был предложен новый алгоритм решения данной задачи, основанный на отображении рассматриваемых функций 2^n-компонентными булевыми векторами и использовании эффективных покомпонентных операций над ними. Ниже этот алгоритм обобщается на случай частичных булевых функций. Тогда произвольную частичную булеву функцию f от n переменных можно представить троичным вектором $\boldsymbol{f}$ с 2^n компонентами, показывающими значения функции на соответствующих наборах значений переменных и упорядоченными традиционным образом, на базе позиционного двоичного кода. Неопределенное значение интерпретируется при этом как произвольное и отображается символом «–». Например, троичный вектор $\boldsymbol{f}$ = 1–01––10 представляет булеву функцию $f(x_1, x_2, x_3)$, принимающую значение 1 на наборах 000, 011 и 110, значение 0 на наборах 010 и 111 и не определенную на наборах 001, 100 и 101.

Рассматривая коэффициенты $f_i(\boldsymbol{u}, \boldsymbol{v})$ дизъюнктивного разложения Шеннона частичной булевой функции $f(\boldsymbol{x})$ по переменным множества $\boldsymbol{w}$, будем представлять их троичными матрицами $\boldsymbol{T}_i$, строки которых соответствуют различным значениям вектора $\boldsymbol{u}$, а столбцы – различным значениям вектора $\boldsymbol{v}$. Элементами этих матриц служат соответствующие компоненты троичного вектора $\boldsymbol{f}$, задающего функцию $f(\boldsymbol{x})$.

Рассмотрим в качестве примера функцию $f(\boldsymbol{x}) = f(x_1, x_2, x_3, x_4, x_5)$, представленную стандартным образом вектором

```
-10101-0 11-10-10  00--1110 -00-11-0

00000000 00000000  11111111 11111111  5
00000000 11111111  00000000 11111111  4
00001111 00001111  00001111 00001111  3
00110011 00110011  00110011 00110011  2
01010101 01010101  01010101 01010101  1
```

(снизу показаны наборы значений аргументов) и принимающую значение 1 на наборах 10000, 11000, 10100, …, значение 0 на наборах 01000, 00100, 11100, … и неопределенное значение на наборах 00000, 01100, 010010, … .

Допустим, что $\boldsymbol{u} = (x_2, x_4)$, $\boldsymbol{w} = (x_5)$ и $\boldsymbol{v} = (x_1, x_3)$. В этом случае два коэффициента разложения функции $f(\boldsymbol{x})$ по единственной переменной множества $\boldsymbol{w}$ удобно представить парой следующих троичных матриц, строки которых соответствуют значениям 00, 01, 10, 11 вектора $\boldsymbol{u}$, а столбцы – таким же значениям вектора $\boldsymbol{v}$:

$$\boldsymbol{T}_0 = \begin{matrix} -101 \\ 01-0 \\ 110- \\ -110 \end{matrix}, \qquad \boldsymbol{T}_1 = \begin{matrix} 0011 \\ --10 \\ -011 \\ 0--0 \end{matrix}.$$

Условие разделимости функции $f(\boldsymbol{x})$ по разбиению $\boldsymbol{u}/\boldsymbol{v}$ сформулируем теперь следующим образом: для каждого коэффициента $f_i(\boldsymbol{u}, \boldsymbol{v})$ возможно такое доопределение соответствующей матрицы $\boldsymbol{T}_i$, при котором ее строки примут не более двух различных значений.

В данном случае это условие выполняется так же, как и в следующем более сложном примере одного коэффициента (слева показана троичная матрица $\boldsymbol{T}_i$, а справа – одно из возможных доопределений):

```
1  1-0---0-     10010100
2  001--01-     00110011
3  ---10--1     00110011
4  10-10-0-     10010100
5  ----00-1     00110011
6  10-1-100     10010100
7  -00-0---     10010100
8  0--1-01-     00110011
```

Сформулированное условие эквивалентно следующему: строки каждой из матриц $\boldsymbol{T}_i$, задающих коэффициенты дизъюнктивного разложения функции $f(\boldsymbol{x})$ по переменным множества $\boldsymbol{w}$, можно разбить на классы A и B, образованные взаимно совместимыми, т. е. неортогональными строками, – они могут стать равными при некотором доопределении.

2. Метод проверки условия разделимости

Проверка матрицы $\boldsymbol{T}_i$ на условие разделимости сводится к проверке графа ортогональности его строк на бихроматичность [7] и может осуществляться методом последовательного расширения классов A и B (вначале пустых), заносящим ортогональные строки в различные классы и проверяющим на совместимость строки, которые попали в один класс.

Данная идея реализуется в следующем итеративном методе, в котором фигурируют классы строк A и B, рассматриваемые как переменные и вначале пустые. Предположим, что условие выполняется. Будем заполнять классы, начав с включения первой строки в класс A и нахождения множества всех ортогональных ей строк. Если это множество несовместно, т. е. содержит некоторую пару взаимно ортогональных строк, исходное предположение принимается за ложное (по правилу *modus tollens*), откуда следует, что функция $f(\boldsymbol{x})$ не декомпозируется по разбиению $\boldsymbol{u}/\boldsymbol{v}$. В противном случае включаем данное множество в класс B и находим все строки, ортогональные этому классу (хотя бы одной из образующих его строк), также проверяя их на совместимость. Совокупность таких строк образует новое значение класса A. После этого отыскиваются строки, ортогональные классу A и, в случае их совместимости, образующие сообща последующее значение класса B. Процесс продолжается аналогичным образом и прекращается, как только все строки матрицы $\boldsymbol{T}_i$ будут распределены по классам A и B. В этом случае примем, что рассматриваемое условие разделимости выполняется.

Метод оказывается эвристическим, гарантируя получение правильного решения лишь при условии связности графа ортогональности строк каждой матрицы $\boldsymbol{T}_i$. Заметим, что при этом число итераций может достигать длины максимального нечетного цикла в графе, что необходимо для проверки графа на бихроматичность.

Проиллюстрируем этот метод на примере той же матрицы, представляя троичными векторами справа от нее получаемые последовательно распределения строк по классам A (значение 1) и B (значение 0). Векторы ниже матрицы задают пересечения строк рассматриваемого на текущем шаге класса, представляя по определению интервалы, образуемые пересечением интервалов, задаваемых строками. Заметим, что если это пересечение оказывается пустым (пересекаемые строки ортогональны), класс несовместен. Рядом показаны номера шагов.

Например, очередные значения класса A находятся на шагах 1 и 5, а класса B – на шагах 3 и 7. Пересечения строк, образующих эти значения, находятся соответственно на шагах 2 и 6 для класса A и на шагах 4 и 8 для класса B:

```
               1 3 5 7
1 1-0---0-     1 1 1 1
2 001--01-     - 0 0 0
3 ---10--1     - - - 0
4 10-10-0-     - - 1 1
5 ----00-1     - - - 0
6 10-1-100     - - 1 1
7 -00-0---     - - 1 1
8 0--1-01-     - 0 0 0

  1-0---0-   2
  0011-01-   4
  10010100   6
  00110011   8
```

Метод достаточно прост, что позволяет реализовывать его параллельно применительно ко всем матрицам $\boldsymbol{T}_i$, соответствующим различным значениям вектора $\boldsymbol{w}$. Это обеспечивает высокое быстродействие его выполнения. Что касается условия связности графа ортогональности строк, оно выполняется почти всегда, нарушаясь лишь при сильной неопределенности функции.

3. Алгоритмизация метода

Данный метод проверки частичной булевой функции на разделимость реализуется излагаемым ниже алгоритмом, который обобщает результаты, полученные в работах [5, 6], на случай частичных булевых функций.

Исходная частичная булева функция $f(\boldsymbol{x})$ от n переменных представляется в этом методе парой всюду определенных булевых функций $f^0(\boldsymbol{x})$ и $f^1(\boldsymbol{x})$, заданных следующим образом:

$$f^0(\boldsymbol{x}) = 1, \text{ если и только если } f(\boldsymbol{x}) = 0;$$

$$f^1(\boldsymbol{x}) = 1, \text{ если и только если } f(\boldsymbol{x}) = 1.$$

Эти функции отображаются 2^n-компонентными булевыми векторами $\boldsymbol{f}^0(\boldsymbol{x})$ и $\boldsymbol{f}^1(\boldsymbol{x})$ соответственно.

Промежуточные данные представляются 2^n-компонентными булевыми векторами $\boldsymbol{h}^0$, $\boldsymbol{h}^1$ и $\boldsymbol{g}$ (им соответствуют булевы функции h^0, h^1 и g), играющими роль переменных и задающими описываемые ниже величины одновременно для всех значений вектора $\boldsymbol{w}$. Вектором $\boldsymbol{g}$ представляется очередное значение класса A либо B (перечень входящих в класс строк, ортогональных другому классу), а пара векторов $\boldsymbol{h}^0$ и $\boldsymbol{h}^1$ служит для представления пересечения этих строк и проверки на совместность. В приводимом ниже примере каждый из этих векторов отображается соответствующей матричной сверткой. Целочисленная переменная k служит для подсчета числа итераций, ограничиваемого параметром K, значение которого выбирается на основе компромисса между требованиями быстродействия и надежности алгоритма.

Наряду с покомпонентными операциями ($\neg$, $\wedge$, $\vee$, $\oplus$) над булевыми векторами в алгоритме применяются операции, в которых взаимодействуют различные компоненты. К их числу относится операция инвертирования функции по переменной x_i

$$\mathrm{N}_{xi} f(x_1, \ldots, x_i, \ldots, x_n) = f(x_1, \ldots, \neg x_i, \ldots, x_n),$$

входящая в состав следующих более сложных операций:

$\mathrm{S}_{xi}^{\vee}$ – дизъюнктивное симметрирование функции по переменной x_i :

$$\mathrm{S}_{xi}^{\vee} f(\boldsymbol{x}) = f(\boldsymbol{x}) \vee \mathrm{N}_{xi} f(\boldsymbol{x}) ;$$

$S_{\boldsymbol{t}}^{\vee}$ – дизъюнктивное симметрирование функции по некоторому подмножеству переменных $\boldsymbol{t} = (t_1, t_2, \ldots, t_m) \subseteq \boldsymbol{x}$:

$$S_{\boldsymbol{t}}^{\vee} f(\boldsymbol{x}) = S_{t1}^{\vee} (S_{t2}^{\vee} \ldots (S_{tm}^{\vee} f(\boldsymbol{x}))\ldots).$$

Через $f(\boldsymbol{u}=\boldsymbol{0})$ в алгоритме обозначена функция, получаемая из $f(\boldsymbol{x})$ присвоением значения 0 всем переменным множества $\boldsymbol{u}$. Она представляет начальный коэффициент f_0 дизъюнктивного разложения функции $f(\boldsymbol{x})$ по множеству переменных $\boldsymbol{u} = (u_1, u_2, \ldots, u_k)$. Ее вычисление можно свести к последовательности подстановок значения 0 на места переменных, образующих множество $\boldsymbol{u}$.

Алгоритм проверки функции $f(\boldsymbol{x})$ на разделимость по разбиению $\boldsymbol{u}/\boldsymbol{v}$:

$\boldsymbol{h}^0 := \boldsymbol{f}^0(\boldsymbol{u}=\boldsymbol{0})$	Получение коэффициента f_0 и его
$\boldsymbol{h}^1 := \boldsymbol{f}^1(\boldsymbol{u}=\boldsymbol{0})$	использование в качестве начального
$k := 0$	значения пары функций h^0 и h^1
1. $\boldsymbol{g} := S_{\boldsymbol{v}}^{\vee}(\boldsymbol{h}^0\boldsymbol{f}^1 \vee \boldsymbol{h}^1\boldsymbol{f}^0)$	Выделение коэффициентов, не равных f_0
$\boldsymbol{h}^0 := S_{\boldsymbol{u}}^{\vee}(\boldsymbol{f}^0\boldsymbol{g})$	Получение их пересечения
$\boldsymbol{h}^1 := S_{\boldsymbol{u}}^{\vee}(\boldsymbol{f}^1\boldsymbol{g})$	
if $(\boldsymbol{h}^0\boldsymbol{h}^1 \neq \boldsymbol{0})$ then No	Проверка на совместность
$k := k + 1$	
if $(k < K)$ go to 1	
Yes	Функция разделима

Выходной полюс Yes достигается в случае разделимости, полюс No – при неразделимости. Знак конъюнкции в формальном описании алгоритма опускается.

Пример. Проиллюстрируем описанный алгоритм на прежнем примере троичной матрицы $\boldsymbol{T}_i$, задающей некоторый коэффициент разложения частичной функции $f(\boldsymbol{x})$ по переменным множества $\boldsymbol{w}$, положив $K = 2$:

$\boldsymbol{f}$	$\boldsymbol{f}^0$	$\boldsymbol{f}^1$	$\boldsymbol{h}^0$	$\boldsymbol{h}^1$	
1-0---0-	00100010	10000000	00100010	10000000	
001--01-	11000100	00100010	00100010	10000000	
---10--1	00001000	00010001	00100010	10000000	
10-10-0-	01001010	10010000	00100010	10000000	
----00-1	00001100	00000001	00100010	10000000	
10-1-100	01000011	10010100	00100010	10000000	
00-0---	01101000	00000000	00100010	10000000	
0--1-01-	10000100	00010010	00100010	10000000	k=0

$\boldsymbol{h}^0\boldsymbol{f}^1 \vee \boldsymbol{h}^1\boldsymbol{f}^0$	$\boldsymbol{g}$	$\boldsymbol{h}^0$	$\boldsymbol{h}^1$	
00000000	00000000	11000100	00110010	
10100010	11111111	11000100	00110010	
00000000	00000000	11000100	00110010	
00000000	00000000	11000100	00110010	
00000000	00000000	11000100	00110010	
00000000	00000000	11000100	00110010	
00000000	00000000	11000100	00110010	
10000010	11111111	11000100	00110010	k=1

$\boldsymbol{h}^0\boldsymbol{f}^1 \vee \boldsymbol{h}^1\boldsymbol{f}^0$	$\boldsymbol{g}$	$\boldsymbol{h}^0$	$\boldsymbol{h}^1$
10000010	11111111	01101011	10010100
00000000	00000000	01101011	10010100

```
00000000    00000000   01101011   10010100
10000010    11111111   01101011   10010100
00000000    00000000   01101011   10010100
10000110    11111111   01101011   10010100
00100000    11111111   01101011   10010100
00000000    00000000   01101011   10010100
```

k=2

Параметр k достигает значения K, при этом конъюнкция $\boldsymbol{h}^0\boldsymbol{h}^1$ остается равной нулю, поэтому рассматриваемый коэффициент признается разделимым по разбиению $\boldsymbol{u}/\boldsymbol{v}$. Напомним, что для признания соответствующей разделимости всей функции f необходимо убедиться в разделимости каждого коэффициента f_i.

Заключение

Проверка булевой функции $f(\boldsymbol{x})$ на разделимость по заданному нестрогому разбиению $\boldsymbol{u}/\boldsymbol{v}$ на множестве аргументов $\boldsymbol{x}$ существенно усложняется в случае частичной определенности функции. Эта задача сводится к проверке на бихроматичность графов ортогональности строк троичных матриц $\boldsymbol{T}_i$, представляющих коэффициенты разложения функции $f(\boldsymbol{x})$ по переменным множества $\boldsymbol{w}$ = =$\boldsymbol{x} \setminus (\boldsymbol{u} \cup \boldsymbol{v})$. Для ускорения процесса решения в предлагаемом методе используется аппарат булевых и троичных векторов и матриц с эффективными покомпонентными операциями над ними.

Список литературы

1. Perkowski, M.A. A survey of literature on function decomposition, Version IV / M.A. Perkowski, Grigiel. – Portland State University, 1995.
2. Поваров, Г.Н. О функциональной разделимости булевых функций / Г.Н. Поваров // Доклады АН СССР. – Т. 94, № 5. – 1954.
3. Ashenhurst, R.L. The decomposition of switching functions / R.L. Ashenhurst // Proc. International Symposium on the Theory of Switching: Part 1. – Cambridge: Harward University Press, 1959. – P. 75–116.
4. Curtis, H.A. Design of switching circuits / H.A. Curtis. – Van Nostrand, Princeton, N. J., 1962.
5. Закревский, А.Д. Алгоритм разделения булевой функции / А.Д. Закревский // Тр. Сибирского физико-технического института. – 1964. – Т. 44. – С. 5-16.
6. Закревский, А.Д. Векторный алгоритм анализа булевой функции на декомпозируемость по заданному разбиению / А.Д. Закревский // Доклады НАН Беларуси. – 2006. – Т. 50, № 5. – С. 28–29.
7. Харари, Ф. Теория графов / Ф. Харари. – М.: Мир, 1973.

Поступила 14.12.06

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: zakr@newman.bas-net.by

A.D. Zakrevskij

DECOMPOSITION OF PARTIAL BOOLEAN FUNCTIONS – CHECKING FOR DECOMPOSABILITY AT A GIVEN PARTITION

A problem of sequential two-block decomposition of partial Boolean functions, generally non-disjunctive, is considered. A novel method is suggested to check a function concerned for decomposability at a given weak partition on the set of arguments. Boolean and ternary vectors and matrices are used for representation of partial Boolean functions with efficient combinatorial operations over them.